AD NUMBER

ADB329088

NEW LIMITATION CHANGE

TO

Approved for public release, distribution unlimited

FROM

Distribution authorized to U.S. Gov't. agencies only; Proprietary Information; NOV 2006. Other requests shall be referred to U.S. Army Research Office, P.O. Box 12211, Research Triangle Park, NC 27709-2211.

AUTHORITY

14 Nov 2006, per document marking

REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE:	3. REPORT TYPE AND DATES COVERED
		Final Report 15-May-2001 - 14-Nov-2006

4. TITLE AND SUBTITLE

Vulnerability Assessment Tools for Complex Information Networks

5. FUNDING NUMBERS

DAAD19-01-1-0610

6. AUTHORS

Christos G. Cassandras, Weibo Gong, David L. Pepyne, Wenke Lee, and Hong Liu, Yu-Chi Ho, Avrom Pfeffer

8. PERFORMING ORGANIZATION REPORT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

Harvard University
Office of Sponsored Research
1350 Massachusetts Ave. Holyoke 727
Cambridge, MA 02138 -

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

42349-MA-CIP.2

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12. DISTRIBUTION AVAILIBILITY STATEMENT

Distribution authorized to U.S. Government Agencies Only, Contains Proprieta

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The abstract is below since many authors do not follow the 200 word limit

14. SUBJECT TERMS

Automated Red Teaming, randomization, intrusion detection, dynamic Bayesian networks, feedback, Stochastic Fluid models, perturbation analysis, wireless networks, epidemic

15. NUMBER OF PAGES

Unknown due to possible attachments

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Report Title

Vulnerability Assessment Tools for Complex Information Networks

ABSTRACT

The specific aims of this research is to develop theories, methodologies, tools, and implementable solutions for modeling, analyzing, designing, and securing information networks against information-based attack. Accomplishments during the current reporting period are documented in 49 publications and 1 patent application and include: New methods for the optimization of complex systems; simulation-based methods for real-time decision making; proof-of-concept implementations of solutions for malware spreading and wireless data-link security; a feedback control approach for defense against DDoS; randomized protocols for managing the performance vs. security trade-off in wireless networks; automated Red Teaming tools and intrusion traceback methods for mobile ad-hoc wireless networks; a new dynamic Bayesian network based approach for detection and estimation in networked environments; and an adaptive defense architecture for fast spreading internet worms. Plans for the coming year will focus on further exploration of optimization, feedback and randomness in security; continued development of methods for security assessment, particularly in wireless settings; completion of the dynamic Bayesian framework for detection and estimation in networks; and a continued exploration of vulnerabilities and methods for military enterprise networks. These efforts will contribute new understanding and new approaches for securing and managing distributed, decentralized command and control systems.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

1. Cassandras, C.G., Sun, G., Panayiotou, C.G., and Wardi, Y., "Perturbation Analysis and Control of Two-Class Stochastic Fluid Models for Communication Networks", IEEE Trans. on Automatic Control, AC-48, 5, pp. 770-782, 2003.
2. Paschalidis, I.C., Y., Liu, Y., Cassandras, C.G., and Panayiotou, C.G., "Inventory Control for Supply Chains with Service Level Constraints: A Synergy between Large Deviations and Perturbation Analysis", Annals of Operations Research, 126, pp. 231-258, 2004.
3. Yu, H., and Cassandras, C.G., "Perturbation Analysis for Production Control and Optimization of Manufacturing Systems", Automatica, Vol. 40, pp. 945-956, 2004.
4. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis of Multiclass Stochastic Fluid Models", J. of Discrete Event Dynamic Systems, Vol. 14, 3, pp. 267-307, 2004.
5. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis and Optimization of Stochastic Flow Networks", IEEE Trans. on Automatic Control, AC-49, 12, pp. 2113-2128, 2004.
6. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Feedback-Controlled Stochastic Flow Systems", IEEE Trans. on Automatic Control, AC-49, 8, pp. 1317-1332, 2004.
7. Panayiotou, C.G., Cassandras, C.G., Sun, G., and Wardi, Y., "Control of Communication Networks Using Infinitesimal Perturbation Analysis of Stochastic Fluid Models", in Advances in Communication Control Networks, Lecture Notes in Control and Information Sciences, Vol. 308, pp. 1-26, (S. Tarbouriech, C.T. Abdallah, and J. Chiasson, Ed's), Springer-Verlag, 2004.
8. Yu, H., and Cassandras, C.G., "A New Paradigm for On-Line Management of Communication Networks with Multiplicative Feedback Control", in Performance Evaluation and Planning Methods for the Next Generation Internet, (A. Girard, B. Sanso, and F. Vazquez-Abad, Ed's), pp. 297-332, Springer-Verlag, 2005.
9. Miao, L., and Cassandras, C.G., "Optimality of Static Control Policies in Some Discrete Event Systems", IEEE Trans. on Automatic Control, AC-50, 9, pp. 1427- 1431, 2005.
10. Cassandras, C.G., and Li, W., "Sensor Networks and Cooperative Control", European Journal of Control, Vol. 11, 4-5, pp. 436-463, 2005.
11. Li, W., and Cassandras, C.G., "A Cooperative Receding Horizon Controller for Multi-Vehicle Uncertain Environments", IEEE Trans. on Automatic Control, AC-51, 2, pp. 242-257, 2006.
12. Li, W., and Cassandras, C.G., "Centralized and Distributed Cooperative Receding Horizon Control of Autonomous Vehicle Missions", J. of Mathematical and Computer Modeling, Vol. 43, 9-10, pp. 1208-1228, 2006.
13. Panayiotou, C.G., and Cassandras, C.G., "Infinitesimal Perturbation Analysis for Make-To-Stock Manufacturing Systems Based on Stochastic Fluid Models", J. of Discrete Event Dynamic Systems, pp. 109-142, 2006.
14. Yu, H., and Cassandras, C.G., "Perturbation Analysis and Feedback Control of Communication Networks Using Stochastic Hybrid Models", Nonlinear Analysis, Vol. 65, 6, pp. 1251-1280, 2006.
15. Miao, L., and Cassandras, C.G., "Receding Horizon Control for a Class of Discrete Event Systems with Real-Time Constraints", to appear in IEEE Trans. on Automatic Control, 2007.
16. Mao, J., Cassandras, C.G., and Zhao, Q., "Optimal Dynamic Voltage Scaling in Power-Limited Systems with Real-Time Constraints", to appear in IEEE Trans. on Mobile Computing, 2007.
17. Prahlad Fogla and Wenke Lee, "q-Gram Matching Using Tree Models", IEEE Transactions on Knowledge and Data Engineering, Vol. 18, No. 4 (April 2006).
18. Guan, X.-H., C. Song, and Y.-C. Ho, "Constrained Ordinal Optimization – A Feasibility Based Approach," submitted to the J. of Discrete Event Dynamic Systems, 2005.
19. Ho, Y.-C., "On Centralized Optimal Control," IEEE Trans. On Automatic Control, Vol. 50, No. 4, pp. 537-539, April 2005.
20. Ho, Y.-C., Q.-C. Zhao, and Q.-S. Jia, "Vector Ordinal Optimization," JOTA, 2005.
21. Jia, Q.-S., Q.-C. Zhao, and Y.-C. Ho, "Selection Rules for Ordinal Optimization," J. of Mathematical and Computer Modeling, 2005.
22. Song, C., X. Guan, Q.-C. Zhao, and Y.-C. Ho, "Machine Learning Approach for Determining Feasible Schedules of a Remanufacturing System," in IEEE Trans. on Automation in Science and Engineering, 2005.
23. Gao, F. and Y.-C.Ho, "Random Approximated Greedy Search for Feature Selection," Asian J. of Control, Vol.6, No. 3, September 2004.
24. Ho, Y.-C., D.L. Pepyne, Q.-C. Zhao, H. Liu, Q. Yu, and B. Dukes, "ProgramID," J. of Discrete Event Dynamic Systems, 2004.
25. Zou, C.C., W. Gong, D. Towsley, and L. Gao, "The Monitoring and Early Detection of Internet Worms," in IEEE/ACM Transactions on Networking.
26. Zou, C.C., D. Towsley, and W. Gong, "On the Performance of Internet Worm Scanning Strategies," in Journal of Performance Evaluation.
27. Lin, S.-Y., C.-H. Lin, and Y.-C. Ho, "An Ordinal Optimization theory Based Algorithm for solving the Optimal Power Flow Problems with Discrete Control Variables," IEEE Transactions on Power Systems, pp. 276-286, February 2004.
28. S.Y. Lin, C.H. Lin, and Y.C. Ho, "An Ordinal Optimization Theory Based Algorithm for solving the Optimal Power Flow Problems with Discrete Control Variables," IEEE Transactions on Power Systems, pp. 276-286, February 2004.
29. Y. Liu and W. Gong, "On Fluid Queueing Systems with Strict Priority," IEEE Transactions on Automatic Control, January 2004.
30. Y. Wu and W. Gong, "Error Analysis of Burst Level Modeling of Active-Idle Sources," in ACM Transactions on Modeling and Simulation, 2004.
31. Yongguang Zhang, Wenke Lee, and Yi-an Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", in ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

Number of Papers published in peer-reviewed journals: 31.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

1. Cassandras, C.G., “Vulnerability Assessment Tools for Complex Information Networks”, ARO Grantee Meeting, Cambridge, MA, May 2002.
2. Cassandras, C.G., “Hybrid Systems, Complexity, and Networking”, NSF-European Union Workshop on Advanced Hybrid Systems Theory for the Control of Networked Systems, Barcelona, Spain, July 2002.
3. Cassandras, C.G., “Joy and Perils of Automation”, NSF National Workshop for High School Teachers of Math and Science, Denver, CO, June 2003.
4. Cassandras, C.G., “Introduction to Hybrid Systems”, Intl. Summer School on Hybrid Systems, Veldhoven, The Netherlands, June 2003.
5. Cassandras, C.G., “Detecting and Reacting to DoS Attacks”, ARO Grantee Meeting, Cambridge, MA, July 2003.
6. Cassandras, C.G., “Cybersecurity”, Cyberposium 2004, Harvard Business School, Cambridge, MA, January 2004.
7. Cassandras, C.G., “Stochastic Fluid Models and Complexity Reduction”, Workshop on Recent Advances in Algebraic Systems and Control Theory, Atlanta, GA, January 2004.
8. Cassandras, C.G., “The Sensor Network Puzzle”, Emerging Technologies Workshop, Boston, MA, May 2004.
9. Cassandras, C.G., “Sensor Networks and Elevator Control for Optimizing Building Evacuation”, NIST Workshop on Building Security, Gaithersburg, MD, June 2004.
10. Cassandras, C.G., and Wu, X., “A Feedback Control Defense Strategy for DoS Computer Attacks”, ARO Grantee Meeting, Cambridge, MA, July 2004.
11. Cassandras, C.G., “A View of Cooperative Control for Autonomous Vehicles and Sensor Networks”, 2005 International Symposium on Intelligent Control, Limassol, Cyprus, June 2005.
12. Cassandras, C.G., “Discrete Event and Hybrid Systems”, IFAC Milestone Session, 16th IFAC World Congress, Prague, Czech Republic, July 2005.
13. Cassandras, C.G., and Wu, X., “Randomized Policies for Exploiting the Security-Performance Tradeoff in Wireless Networks”, ARO Grantee Meeting, Cambridge, MA, August 2005.
14. Cassandras, C.G., “Distributed Cooperative Coverage Control Using Sensor Networks”, Workshop on Distributed Sensor Networks, Los Alamos, NM, March 2006.
15. Cassandras, C.G., and Zhuang, S., "Dynamic Voltage Scaling for Power-Limited Systems with Hard and Soft Real-Time Tasks", 2006 INFORMS Annual Meeting, Pittsburgh, PA, November 2006.

Number of Presentations: 15.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

1. Cassandras, C.G., "From Discrete Event to Hybrid Systems", Proc. of 2002 Intl. Workshop on Discrete Event Systems, pp. 3-8, October 2002.
2. Cassandras, C.G., "Stochastic Fluid Models for Communication Networks", Proc. of 17th Intl. Symposium on Computer and Information Sciences, pp. 8-11, October 2002.
3. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis of a Multiclass Stochastic Fluid Model with Finite Buffer Capacity", Proc. of 41st IEEE Conf. Decision and Control, pp. 2171-2176, Dec. 2002.
4. Cassandras, C.G., and Mookherjee, R., "Receding Horizon Control for a Class of Hybrid Systems with Event Uncertainties", Proc. of 2003 American Control Conf., pp. 5197-5202, June 2003.
5. Cassandras, C.G., and Mookherjee, R., "Properties of Receding Horizon Controllers for Some Hybrid Systems with Event Uncertainties", Proc. 2003 IFAC Conf. on Analysis and Design of Hybrid Systems, pp. 413-418, June 2003.
6. Cassandras, C.G., and Mookherjee, R., "Receding Horizon Optimal Control for Some Stochastic Hybrid Systems", Proc. of 42nd IEEE Conf. Decision and Control, pp. 2162-2167, Dec. 2003.
7. Sun, G., Cassandras, C.G., Wardi, Y., and Panayiotou, C.G., "Perturbation Analysis of Stochastic Flow Networks", Proc. of 42nd IEEE Conf. Decision and Control, pp. 4831-4836, Dec. 2003.
8. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Feedback-Controlled Stochastic Flow Systems", Proc. of 42nd IEEE Conf. Decision and Control, pp. 6277-6282, Dec. 2003.
9. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Stochastic Fluid Models with Multiplicative Feedback", Proc. of 2004 American Control Conf., pp. 5734-5739, June 2004.
10. Panayiotou, C.G., and Cassandras, C.G., "Infinitesimal Perturbation Analysis for Make-To-Stock Manufacturing Systems Based on Stochastic Fluid Models", Proc. of 2004 Intl. Workshop on Discrete Event Systems, pp. 247-252, Sep. 2004.
11. Wu, X., and Cassandras, C.G., "A Feeback Control Defense Strategy for Denial-of-Service Attacks", Proc. of 43rd IEEE Conf. Decision and Control, pp. 105-110, Dec. 2004.
12. Li, W., and Cassandras, C.G., "Stability Properties of a Receding Horizon Contoller for Cooperating UAVs", Proc. of 43rd IEEE Conf. Decision and Control, pp. 2905-2910, Dec. 2004.
13. Mao, J., Zhao, Q., and Cassandras, C.G., "Optimal Dynamic Voltage Scaling in Power-Limited Systems with Real-Time Constraints", Proc. of 43rd IEEE Conf. Decision and Control, pp. 1472-1477, Dec. 2004.
14. Yu, H., and Cassandras, C.G., "Multiplicative Feedback Control in Communication Networks Using Stochastic Flow Models", Proc. of 43rd IEEE Conf. Decision and Control, pp. 557-562, Dec. 2004.
15. Li, W., and Cassandras, C.G., "A Minimum-Power Wireless Sensor Network Self-Deployment Scheme", in Proc. of IEEE Wireless Communications and Networking Conference, 2005.
16. Miao, L., and Cassandras, C.G., "Optimality of Static Control Policies in Some Discrete Event Systems", Proc. of 2005 American Control Conf., pp. 1186-1191, June 2005.
17. Cassandras, C.G., and Li, W., "Cooperative Control Problems in the Deployment of Sensor Networks", in Proc. of Workshop on Modeling and Control of Complex Systems, June 2005.
18. Yu, H., and Cassandras, C.G., "Perturbation Analysis and Feedback Control of Communication Networks Using Stochastic Hybrid Models", in Proc. of 16th IFAC World Congress, July 2005.
19. Miao, L., and Cassandras, C.G., "Receding Horizon Control for a Class of Discrete Event Systems with Real-Time Constraints", Proc. of 44th IEEE Conf. Decision and Control, pp. 7714-7719, Dec. 2005.
20. Li, W., and Cassandras, C.G., "Distributed Cooperative Coverage Control of
21. Sensor Networks", Proc. of 44th IEEE Conf. Decision and Control, pp. 2542-2547, Dec. 2005.
22. Wu, X, and Cassandras, C.G., "A Maximum Time Optimal Control Approach to
23. Routing in Sensor Networks", Proc. of 44th IEEE Conf. Decision and Control, pp. 1137-1142, Dec. 2005.
24. Miao, L.., and Cassandras, C.G., "Optimal Transmission Scheduling for Energy-Efficient Wireless Networks", Proc. of IEEE INFOCOM'06, April 2006.
25. Mao, J., and Cassandras, C.G., "Optimal Control of Two-Stage Discrete Event Systems with Real-Time Constraints", Proc. of 2006 Intl. Workshop on Discrete Event Systems, pp. 145-150, July 2006.
26. Mao, J., and Cassandras, C.G., "Optimal Control of Multi-Stage Discrete Event Systems with Real-Time Constraints", Proc. of 45th IEEE Conf. Decision and Control, pp. 1057-1062, Dec. 2006.
27. Ning, X., and Cassandras, C.G., "Dynamic Sleep Time Control in Event Driven Wireless Sensor Networks", to appear in Proc. of 45th IEEE Conf. Decision and Control, pp. 2722-2727, Dec. 2006.
28. Miao, L., and Cassandras, C.G., "Structural Properties of Optimal Uplink Transmission Scheduling in Energy-Efficient Wireless Networks with Real-Time Constraints", Proc. of 45th IEEE Conf. Decision and Control, pp. 2997-3002, Dec. 2006.
29. Y. Huang, W. Gong, D. Gupta, "MCMSDA: A Multi-Channel Multi-Sector Directional Antenna Wireless Lan", in proceeding of IEEE WOWMOM 2006, Buffalo, NY, June 26-29, 2006.
30. Monirul Sharif, George Riley, and Wenke Lee, "Comparative Study between Analytical Models and Packet-Level Worm Simulations", in Proceedings of The 19th Workshop on Parallel and Distributed Simulation (PADS 2005), Monterey, CA, June 2005.
31. Y. Huang, W. Gong, D. Gupta, "Architecture and scheduling algorithm for a multi-channel wireless infrastructure network with diversity management layer", in proceeding of 44th IEEE Conference on Decision and Control, Dec, 2005.

32. Chen, X., H. Bai, L. Xia, and Y.C. Ho, “Target Detection in Randomly Distributed Sensor Networks,” in preparation.
33. Huang Y., and W. Lee, “Hotspot-Based Traceback for Mobile Ad Hoc Networks,” Proc. of the 2005 ACM Workshop on Wireless Security (WiSe 2005), Cologne, Germany, September 2005.
34. Pfeffer, A., and T. Tai, “Asynchronous Dynamic Bayesian Networks,” Proc. of the 20st Conf. on Uncertainty in Artificial Intelligence, 2005.
35. Zou, C.C., D. Towsley, W. Gong, and S. Cai, “Routing Worm: A Fast, Selective Attack Worm based on IP Address Information,” 19th ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation (PADS'05), June 2005.
36. Ho, Y.-C. and D.L. Pepyne, "A Conceptual Framework for Optimization and Distributed Intelligence," Proc. of the 43rd IEEE Conf. on Decision and Control, December 2004.
37. Zou, C.C., N. Duffield, D. Towsley, and W. Gong. "Adaptive Defence Against Various Network Attacks," SRUTI: Steps to Reducing Unwanted Traffic on the Internet, July 2005.
38. Zhang, Y., Y. Huang, and W. Lee, “An Extensible Environment for Evaluating Secure MANET,” Proc. of the 1st IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, September 2005.
39. Zou, C.C., D. Towsley, and W. Gong, "Email Worm Modeling and Defense,”13th International Conference on Computer Communications and Networks (ICCCN'04), October 2004.
40. S. Cai, L. Gao, W. Gong, and W.-Q. Xu, "On Generating Internet Hierarchical Topology," in the Proceedings of IEEE Conference on Decision and Control (CDC) 2004.
41. S. Cai, Y. Liu and W. Gong, "Client-Controlled Slow TCP and Denial of Service,” in Proceedings of IEEE Conference on Decision and Control (CDC) 2004.
42. D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levin, and H. Owen, “HoneyStat: Local Worm Detection Using Honeypots,” in Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), French Riviera, France, September 2004.
43. H.H. Feng, J.T. Giffin, Y. Huang, S. Jha, W. Lee, and B.P. Miller, “Formalizing Sensitivity in Static Analysis for Intrusion Detection,” in Proceedings of The 2004 IEEE Symposium on Security and Privacy, Oakland, CA, May 2004.
44. G. Gu, D. Dagon, X. Qin, M.I. Sharif, W. Lee, and G.F. Riley, “Worm Detection, Early Warning, and Response Based on Local Victim Information”, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC 2004), Tucson, Arizona, December 2004.
45. Ho, Y.-C. and D.L. Pepyne, "A Conceptual Framework for Optimization and Distributed Intelligence," 43rd IEEE Conference on Decision and Control, 2004.
46. Y. Huang and W. Lee, “Attack Analysis and Detection for Ad Hoc Routing Protocols,” in Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), French Riviera, France, September 2004.
47. D. Pepyne, J. Hu, and W. Gong, "User Profiling for Computer Security," Proc. of the American Control Conference, Boston, MA, June 30-July 2, 2004.
48. G.F. Riley, M.I. Sharif, and W. Lee. “Simulating Internet Worms”, Proc. of the 12th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Volendam, The Netherlands, October 2004.
49. C.C. Zou, D. Towsley and W. Gong. "Email Worm Modeling and Defense,” in 13th International Conference on Computer Communications and Networks (ICCCN'04), October 11-13, Chicago, 2004.
50. Zhou, T., Q. Yu, and H. Liu, “Comparison of Wireless Security Protocols,” Proc. of the Int. Conf. on Computer, Communication and Control Technologies (CCCT’03), Orlando, FL, 2003.
51. C. Crick and A. Pfeffer, “Loopy Belief Propagation as a Basis for Communication in Sensor Networks,” Conf. on Uncertainty in AI, 2003.
52. A. Shrestha, L. Xing, and H. Liu, “Application Communication Reliability of Wireless Sensor Networks”, Proceedings of The 12th ISSAT International Conference on Reliability and Quality in Design, August 3-5, 2006, Chicago, Illinois.
53. Q. Yu and H. Liu, “Denial-of-Service Countermeasure with Immunization and Regulation,” IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005), Athens, Greece, 5-9 September 2005.
54. R. Suryanarayanan, L. Xing, and H. Liu, "Delay Reliability Analysis of a DiffServ Router," Proceedings of IASTED International Conference on Communications and Computer Networks, Cambridge, MA, 8-10 November 2004, pp. 362-367.
55. Q. Yu, S. Sharma, and H. Liu, "Handling Denial-of-Service Attacks with Quality-of-Service Framework," CNIS 2003: IASTED International Conference on Communication, Network, and Information Security, December 10 - December 12, 2003, New York, New York.
56. T. Zhou, Q. Yu, and H. Liu, "Comparison of Wireless Security Protocols," CCCT 2003: International Conference on Computer, Communication and Control Technologies, July 31 - August 2, 2003, Orlando, Florida.

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts): 56

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

NAME	PERCENT_SUPPORTED	
Kirk Wesselowski		No
Xiaoyi Wu		No
Shixin Zhuang		No
Xu Ning		No
QingShan Jia		No
Brenda Ng		No
Qin Yu		No
Yi-an Huang		No
Paul Royal		No
Takehiro Takahashi		No
Cliff Zou		No
Yong Huang		No
Jie Sun		No
Sheng Xiao		No
Yan Cai		No
Songlin Cai		No
Hanping Feng		No
Jonathan Lee		No
X.C. Lin		No
Jinghua Hu		No
Tong Liu		No
Yujing Wu		No
Haining Yu		No
Gang Sun		No
Ying Liu		No
FTE Equivalent:		
Total Number:	**25**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED	
David Pepyne		No
FTE Equivalent:		
Total Number:	**1**	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Yu-Chi (Larry) Ho		Yes
Avrom (Avi) Pfeffer		No
Christos G. Cassandras		No
Weibo Gong		No
Wenke Lee		No
Hong Liu		No
FTE Equivalent:		
Total Number:	**6**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	
Robert Edmunds		No
Mitch Halpin		No
FTE Equivalent:		
Total Number:	**2**	

Names of Personnel receiving masters degrees

NAME
Total Number:

Names of personnel receiving PHDs

NAME		
Jonathan Lee	No	
X.C. Lin	No	
Qing-Shan Jia	No	
Kirk Wesselowski	No	
Changchun Zou	No	
Hanping Feng	No	
Songlin Cai	No	
Xiaoyi Wu	No	
Yi-an Huang	No	
Gang Sun	No	
Haining Yu	No	
Xiaoyi Wu	No	
Total Number:	**12**	

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	31 Dec 2006	Final Report, 15 May 01 – 14 Nov 06

4. TITLE AND SUBTITLE
Vulnerability Assessment Tools for Complex Information Networks
FINAL REPORT TITLE
Vulnerability Assessment Tools for Complex Information Networks

5. FUNDING NUMBERS
DAAD19-01-1-0610

6. AUTHOR(S)
Yu-Chi Ho, Avrom Pfeffer, Christos G. Cassandras, Weibo Gong,
David L. Pepyne, Wenke Lee, and Hong Liu

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Massachusetts - Amherst
Office of Grant & Contract Admin.
408 Goodell Building
Amherst, MA 010033285

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
42349MACIP

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE
.

13. ABSTRACT (Maximum 200 words)

The **specific aims** of this research project are to develop theories, methodologies, tools, and implementable solutions for modeling, analyzing, designing, and securing information networks against information-based attack. **Accomplishments** over the project period are documented in 31 journal and 56 conference publications and include: Theoretical examination of security limits in complex systems; general network defense principles for vulnerability reduction by amplification of local security measures; modeling and analysis of worms and viruses; Kalman filtering and feedback control for quick detection and mitigation of worms; feedback defense system for DDoS and worm attacks and a theory for its analysis and tuning; user profiling for insider attack; self-organizing, self-learning methods for intrusion detection in mobile ad-hoc networks (MANET); and a probabilistic belief propagation approach for early detection of network attacks.

14. SUBJECT TERMS
Vulnerability models, randomization, intrusion/misuse detection, distributed resource allocation, propagation models, information-based attack, threat models, probabilistic models, wireless security

15. NUMBER OF PAGES
18

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**	**UL**

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

REPORT DOCUMENTATION PAGE (SF298)
(Continuation Sheet)

(1) Foreword (optional)

(2) Table of Contents (if report is more than 10 pages)

(3) List of Appendixes, Illustrations and Tables (if applicable)

(4) Statement of the problem studied

- **Early detection of distributed network attacks.** If we look at the incidence curve of an attack, we see that early detection can make a big difference in being able to prevent a large amount of damage. Such an attack can only be detected in distributed way. Limited evidence is available at individual nodes. A single node may have enough evidence to make it “slightly suspicious”, but not enough to initiate a response. However, when many nodes are slightly suspicious their beliefs can be integrated to produce a high level of suspicion. The problem we have studied is: how can small distributed pieces of evidence be combined in a coherent way? Any algorithm for doing this must be fully distributed and cannot rely on centralized control.

- **A systematic analysis of vulnerabilities (possible attacks) on wireless ad-hoc routing protocols.** Bbased on this analysis, the development of intrusion detection algorithms for mobile ad-hoc networks (MANETs).

- **An Extensible Environment for Evaluating Secure MANET.** We propose a software framework for a development and testing environment to automate the complex process of developing and evaluating secure MANET (mobile adhoc networks) in real systems. This process involves careful design of attack test cases and security countermeasures, as well as meaningful performance measurements to evaluate both the impact of attacks and the performance of security solutions. We also describe a system implementation in the secure MANET routing domain. This environment includes the following three major features. First, the environment is built upon a wireless network emulation tool to support repeatable experimentation. Second, it adds an attack emulation layer with necessary API for easy development and execution of attack test cases. Third, the extensible attack library includes a full set of basic attacks at its core and a way to compose complex attacks from the atomic elements. We show the development of an Intrusion Detection System (IDS) as a case study. The platform can greatly facilitate the development of security solutions on MANET.

- **Secure key exchange in wireless environment and the manageable security infrastructure.** We proposed a very counter-intuitive secure key exchange scheme which utilizes physical layer properties. It provides extra gain on security performance and can defend any future technology advancement. The theoretical analysis for the basic scheme is accomplished. We are now designing and implementing experimental environments to verify this scheme as well as to measure its practical performance. We also plan to expand this novel idea to related areas of interests. For manageable security infrastructure, we are researching on the hieratical topology. The technology feasibility and scalability are most concerned parts during our research. We achieved a conclusion that once the topology is not favorable to management, there is no security could be implemented. Our proposed solution would explicitly include segmented management capability instead of irresponsibly bet all security on the peer-to-peer fantasy.

- **Enhance our prototypes for the two security solutions, ProgramID and SPRiNG, and educate public about security awareness in Internet and computer usage.** Based on the feedback from last year's survey and experiments on the prototypes among our undergraduate and graduate students, we improved the implementation of our prototypes. Our study demonstrated the effectiveness of the ideas and testified the feasibility of the implementations. We went to K-12 schools, public and private, to teach user safety of Internet and computer. We also take the opportunity to attract high school girls into the field of information technology.

- **Defending against Distributed Denial-of-Service (DOS) attacks.** We chose to concentrate on DoS attacks because they are among the simplest to generate, yet have proven extremely hard to protect against. No automatic means of protection exist for such attacks; instead, network operators are forced to track and manually analyze traffic flows and performance data in order to locate the source(s) of an attack and counteract it. Conventional means of protection (e.g., firewalls) cannot stop a DoS attack. Moreover, emerging networks (including wireless and ad hoc) are likely to be even more vulnerable to this form of attack. We have sought to develop effective, simple strategies for automatically detecting and reacting to DoS attacks, particularly those that are launched in a distributed fashion (i.e., from multiple sources).

- **Randomized policies for exploiting the security-performance tradeoff in wireless networks.** We have addressed the issue of using randomized network operating policies for security purposes. The motivation comes from observing that a random deviation from an optimal network operating policy (e.g., for routing or scheduling), while obviously reducing the level of performance, also reduces the effect of attacks because it makes network behavior less predictable to an attacker. A key issue then is to quantify this tradeoff and explore whether it can work to our advantage. We have determined that at least in some simple tractable cases this tradeoff is such that while performance is relatively insensitive to random deviations from a known optimal policy under normal conditions, it is significantly better under attack. We have pursued this line of research in wireless networks which are notoriously vulnerable to simple attacks when operating with deterministic routing policies (i.e., policies where source nodes send data through one or more fixed paths).

- **Developing appropriate abstraction models for fast decision-making.** One of the difficulties in controlling large-scale networks is that their analysis becomes highly complex. Even when employing discrete event simulation methods, the need to track the dynamics of the network on an event-by-event basis results in prohibitively low processing speeds. When real-time decisions are needed (which is typically the case when an attack occurs) this slows down any decision-making process. We have worked towards developing models at the “right” abstraction level in the sense that the essential features of the network behavior are captured while maintaining a desirable level of simplicity.

- **Automated Red Teaming for Mobile Ad-Hoc Networks (MANETs).** S-MobiEmu, an extensible environment for evaluating security technologies for MANETs is developed. S-MobiEmu is based on MobiEmu, an emulation environment for MANETs. S-MobiEmu implements a set of basic attacks, which can be combined to implement complex attack scenarios. S-MobiEmu also includes a library of performance measures. We have used S-MobiEmu to build a test environment for evaluating intrusion detection algorithms for MANETs (see **Zhang, Huang, and Lee, 2005**). This work shows that it is possible to build an extensible and comprehensive environment for evaluating proposed MANET security solutions. Key advantages of S-MobiEmu are: (*a*) it is an emulation environment, and as a result, any upper layer applications can run on it without changes; (*b*) it has an extensive set of basic attacks and can easily be combined to implement more complex attack scenarios; and (*c*) it has a set of comprehensive security performance measures.

- **Intrusion trace back in MANETs.** In addition to the above work, we developed intrusion trace back techniques for MANETs. In our protocol, a node can query its neighbors about a packet involved in an attack. Each neighbor checks this packet against record of received packets. If there is a match, the neighbor continues the trace back via queries to its neighbors, and so on back towards the source. The innovative feature of our

protocol is the use of a Bloom filter for maintaining information about received packets. A Bloom filter is a probabilistic data structure used to test whether or not an element is a member of a set. While they risk false positives, Bloom filters have a strong space advantage over other data structures. While other data structures – such as search trees, hash tables, arrays, or linked lists – can require storing the packets themselves, a Bloom filter can require the storage of only a few bits per element (the number of bits depending on the desired false positive rate). This compact storage makes the Bloom filter ideal for storing packets in high-speed networks. Another advantage of the Bloom filter is that the time needed to check whether an item is in the set is a fixed constant that is completely independent of the number of items already in the set. In hardware the Bloom filter can be parallelized. We showed that for several important classes of attacks, our simple Bloom filter based trace back protocol is able to locate an attacker or victim to its immediate neighborhood (see **Huang and Lee, 2005**).

- **Advanced Bayesian networks for distributed monitoring, vulnerability assessment, and dynamic defense.** Effectively detecting network security attacks cannot be done by nodes acting independently of each other. The nodes must communicate with each other in order to monitor the state of the network as a whole. We have developed an object-oriented Bayesian network model for detecting attacks. The model has three layers: the individual node layer, which uses intrusion detection systems to help detect the state of individual nodes; the subnet layer that combines information from the individual nodes to detect attacks on a site; and the network layer, which combines all the information to detect attacks on the network as a whole. The key problem is state estimation: to estimate the current state of the network based on the collective evidence from all nodes in the network.

  In earlier work (**Crick and Pfeffer, 2003**), we developed an initial approach to the state estimation problem. The approach was based on belief propagation – each node of the network would send a message to its neighbors summarizing its own beliefs, and then nodes would combine the messages received from neighbors to update their beliefs. We demonstrated that this approach is robust. However it is inadequate for network monitoring because it does not take into account the dynamics of the system – the fact that the state of the network at one time point is closely related to the state at the previous time point. In order to perform effective state estimation in dynamic environments, it is necessary to model system dynamics and integrate evidence from the past together with current observations in forming beliefs.

  In later work (**Pfeffer and Tai, 2005**), we have developed a new approach to distributed, asynchronous state estimation that does take into account system dynamics. The approach is again based on belief propagation. However, to ensure that evidence from different time points is integrated, each node maintains a history of its instantiations at different points in time. Each of these historical instantiations is involved in the message passing process.

  For the representation we use Continuous Time Bayesian Networks. These models represent the dynamics of the system in continuous time and can be used to compute changes in the state of the system over any time interval. This is important because the nodes update asynchronously, and the time between updates of a node can be arbitrary. We developed algorithms for computing beliefs at all the nodes in the network. These algorithms require converting the representation of Continuous Time Bayesian Networks into that of discrete-time Dynamic Bayesian Networks in order to perform the belief propagation. We have proposed two methods for performing this conversion.

  Our experimental results are very promising. We have compared our approach with an existing approach to state estimation called Factored Frontier. Factored Frontier is a synchronous algorithm; therefore it is not suited for network monitoring. Nevertheless it provides the closest point of comparison since our framework is the first asynchronous monitoring framework for Bayesian networks. One might expect that because Factored Frontier is synchronous, its monitoring accuracy will be better than our asynchronous algorithm. In fact the opposite is true: our algorithm significantly outperforms Factored Frontier. An important next step in our research is to understand why this is so.

- **Internet Worm Detection and Defense.** We have developed efficient algorithms for detecting fast spreading Internet worms and corresponding adaptive methods for defense against them. These methods are described in publications in *IEEE/ACM Transactions on Networking* and prestigious network security conferences. We also, jointly with AT&T researchers, filed a patent application on our adaptive malware detection and defense method. Some of this design is described in (**Zou, Duffield, Towsley, and Gong, 2005**).

- **Technologies for wireless mesh networks.** Over the past year we started work on two new areas related to wireless networks. The first involves the use of ad-hoc sensor networks for intrusion detection and area coverage (**Chen, Bai, Xia, and Ho**). The second involves a study of wireless mesh networks. Wireless mesh

networks is a new technology with both military as well as civilian application. Because they are so flexible, wireless mesh networks are expected to become very important. But as they become more important, they could also well become the most vulnerable part of a network. Assessing the vulnerability and reducing the vulnerability of such networks will present significant challenges, some of which we have begun to investigate.

Since security is often at odds with performance, we propose that one should boost network performance at the same time that security is being tightened. Particular ideas that we are exploring in this direction include (*a*) using multipath TCP to improve the performance of wireless mesh networks and wireless communication security; (*b*) using TCP relay to improve the efficiency and reliability of wireless mesh networks; (*c*) using physical layer features to provide secure key exchange among authorized users and form testable perimeter protections.

(5) Summary of the most important results

The broad objectives of this research project are to address both short-term and long-term information network security issues. Short-term issues relate to making today's information networks more secure. Long-term issues relate to how to design secure information networks from scratch when one has the option to do so, as, for example, when an ad hoc network is assembled for a specific military operation. To address these broad objectives our research centers on the development of methodologies, tools, and implementable solutions for modeling, analyzing, designing, and securing information networks against information-based attack. The intent of these tools and solutions is to provide three basic services: A measure of the overall level of security to allow network administrators to determine ***when*** a security problem exists; Identification of actual, possible, or potential areas of vulnerability to allow network administrators to pinpoint ***where*** security problems exist; and methods for improving security posture with static and dynamic resource allocation to allow network administrators to determine ***how*** to respond to security incidents and threats. Traditionally these vulnerability assessment services were provided by human penetration testing (Red Teams). However, the many drawbacks of Red Teaming (cost, invasiveness, lack of continuous real-time protection, bias due to the team's experience, and the risk of damage and system compromise) motivate the development of automated and real-time self-diagnosis. Our **approach** is based on the extension of systems engineering and control theoretic tools to the security domain; the identification and exploitation of architectural structures that facilitate security modeling testing and management decomposition; the application of optimization and feedback control to complex security problems; and the determination of the fundamental theoretical limits to performance and security in complex systems.

During this research project, we have accomplished much towards accomplishing the above research objectives. Specifically, we have demonstrable results – documented in 2 book chapters, 31 journal articles, and 56 conference papers, extensive simulation-based data, and demo software – in the following areas,

- **An attack analysis approach for MANET**: The first step is to identify the normal and anomalous basic events in ad-hoc routing. The specification of the routing protocol is then expressed as a finite-state automaton in terms of normal basic events in routing operations. The next step is to define taxonomy of possible attacks on authenticity, confidentiality, integrity, and availability to analyze the anomalous basic events will be resulted from each attack.

  Based on the attack taxonomy, an intrusion detection system can be constructed as follows. There are attacks that can be detected as violations of the specification of the routing protocol and the anomalous basic events are events that are not allowed in the finite-state automaton. Other attacks result in abnormal sequences or frequency of legitimate basic events. For these attacks, a machine-learning based approaches is used to train a normal profile to detect such anomalies.

  We applied the above attack analysis approach and developed intrusion detection algorithms for two routing protocols: AODV and OLSR. The results showed that our systems can detect most of attacks (known to date) with above 85% detection rate and below 5% false alarm rate.

- **Vulnerability modeling:** We have identified plausible attack scenarios and developed models for specific types of attacks including cascading propagation of Internet worms, email viruses, and congestion (Denial-of-Service attack). The Internet worm and virus models are actually based on the graphical MIMIC (Modular Interconnection of Markov Interacting Chains) framework described in our original proposal. With these models we can detect when a network is under attack and we can devise strategies for mitigating the attack. We have also identified specific vulnerabilities, including vulnerabilities in email power-law topologies, wireless data channels, and routing

in ad-hoc wireless protocols. To combat these vulnerabilities, we are devising specific detection and response techniques.

- **Data Mining:** The evidence for network attacks resides in the data stored in the network and flowing over the links of the network. We have explored many sensor technologies and sensor fusion technologies for mining and extracting attack indicators from network and host data. Key results include intrusion and misuse detection methods for both wired and wireless infrastructures and an advanced Bayesian framework for network-wide monitoring and detection.

- **Threat Modeling:** Because the number of possible attacks on a network is huge (and ever-growing), the models and methods we have developed have focused not on individual attacks but rather on different attack *scenarios*, e.g., Internet worms and viruses, denial-of-service attacks, and routing protocols in ad hoc wireless networks. This allows for the design of proactive methods effective against broad *classes* of individual attacks and vulnerabilities, both known and yet to be exploited.

- **Resource Allocation/Feedback Control:** We take the novel view of network security as an optimization and feedback control problem to allocate security resources and mete out response to attacks with a degree of aggressiveness that adapts to attack severity. Given that many attacks (e.g., worms, viruses, denial-of-service) simply cannot be effectively detected or mitigated by human operators, the models and methods we are developing are designed with the ultimate purpose of devising approaches capable of real-time automated response.

- **Performance and Security Limits of Complex Systems:** Our work on the No Free Lunch Theorem (NFLT) demonstrated that there are fundamental limits to the performance and security of increasingly complex systems. One key conclusion from this work is that system complexity is closely tied to its structure and architecture. Thus, this theoretical foundational research reinforces practical conclusions reached via experience. For example, many schemes that do not scale up well can be made more scalable when used on subunits of a hierarchical structure (divide and conquer is the only antidote against exponential growth). Another key conclusion from the NFLT is the need for *simple decentralized* solutions (emphasis on simple) to complex system problems (versus single all-encompassing grand solutions). This is a conclusion reinforced by the many successful examples of simple strategies for "coping with complexity" found in nature (e.g., swarm intelligence of insect colonies, robustness of immune systems) and in everyday human societies (e.g., social trust networks).

- **General Defense Strategies in Networked Systems:** In a network consisting of a large number of agents (e.g., users, computers, routers), simple actions by each individual agent can lead to a gradual reduction in overall network vulnerability. We refer to this as the "think global, act local" (TGAL) principle. In (**Ho, Pepyne, Zhao, Liu, Yu and Dukes, 2004**) we explored one such TGAL idea by showing how a simple change in the behavior of even a fraction of the users on a large network can lead to a gradual global improvement in the resistance of the network to software vulnerability exploits (e.g., malicious email attachments). The basic idea is to give users a simple means to control what programs are allowed to run on their personal computers. By giving users the capability to identify and regulate what programs run on their computers, we put in place the basis of an infrastructure through which users acting *locally* in a completely decentralized way can produce a gradual improvement in the *global* security of a network. A practical demonstration is implemented in **(Ho, Pepyne, Zhao, Liu, Yu and Dukes, 2004**). General questions remain about the most effective ways to get the local actions of individuals to multiply to have measurable system level global effect. This is both a problem dependent and architectural issue that we will continue studying in our research towards more defendable architectures.

- **Dynamic Detection and Mitigation of Internet Worms and Viruses:** Worms and virus attacks have rapidly become one of the biggest threats to network security. While early worms and viruses were largely nuisances because they did not carry destructive payloads, this has changed, with worms and viruses now installing spyware and backdoors that attackers later use for remote monitoring and exploitation. As our information infrastructures continue to converge, another danger of worms and viruses is that their effects are spreading over to disrupt other essential services such as ATM machines, 911 emergency services, and in one case a nuclear power plant SCADA system. There have also been changes in worm and virus "technologies", such as the new generation of "flash" worms that can spread throughout the Internet, not in hours as was the case just a few years ago, but in minutes as with the "SQL Slammer" worm of 2003. The potential for worms and viruses to rapidly and severely disrupt our civilian and military infrastructures is clear. Moreover, the extremely rapidity with which worms and viruses can spread across management domains makes it clear that *manual intervention by network administrators to control worms and email viruses is simply not possible, making quick-acting automated approaches essential to information infrastructure protection*.

In addressing the threat of worms and viruses, our goal is to develop strategies capable of providing accurate and timely defense for individual (local) networks on one hand and to supply high-quality alert data for global (Internet) detection/mitigation systems. Using concepts from systems and control theory, we have developed dynamic models for the spread of Internet worms and email viruses. Based on these dynamic models we have proposed a Kalman filtering based approach for the early detection of the "outbreak" of Internet worms. Once detected, we have devised a feedback control approach involving "dynamic quarantine" to mitigate (slow or stop if possible) the worm's continued spread.

- A modeling study of email worm propagation on the logical network defined by email address relationships. We find that while email worms spread more quickly on a power law topology than on a small world topology or a random graph topology, immunization defense is more effective on a power law topology than on the other two (**C.C. Zou, D. Towsley, and W. Gong, 2004**).

- Presentation of a "Firewall Network System" to protect military enterprise networks from infection by scan-based worms. The basic idea of the Firewall Network System is to impose a hierarchical structure on an enterprise network and then quarantines worms by blocking the worm scanning and infection traffic from going across the major subunits in the hierarchy (**C.C. Zou, D. Towsley, and W. Gong, 2004**).

- Proposal of a user-based feedback email worm defense system for protection of enterprise networks from infection by mass-mailing email worms (**C.C. Zou, W. Gong, and D. Towsley, 2004**).

- Development of a worm detection algorithm based on local victim information. This algorithm first detects a host with infection-like activities, and then analyzes the scanning behavior of the host to determine if it is indeed a worm victim (**Gu et al. 2004**).

- Development of a honeynet system to automatically record suspicious events, analyze alerts using logistic regression to detect worms, and capture worm code for signature extraction. Experiments on simulations and data of actual worm outbreaks (e.g., Blaster) show that our approaches can detect new (zero-day) worms more accurately and faster than existing algorithms (**Dagon et al. 2004**)

- Development of an analytical model of worm propagation and a large-scale packet-level worm simulation environment to evaluate the effectiveness of worm detection and response strategies. (**Gu et al. 2004; Riley et al. 2004**)

- **An automated feedback control-based defense strategy for Distributed Denial-of-Service Attacks:** Our work initially focused on developing models of a typical DoS attack and exploring the use of simple feedback control mechanisms for minimizing their effect and subsequently tracking down their source(s). This approach eventually led to an explicit defense scheme (Wu and Cassandras, 2005) based on the following steps:

  Step 1: Detect when there is a potential DoS attack at a "victim node" by sensing that a buffer exceeds some threshold T1. At this point, the flow with the most packets in the buffer is labeled as a "suspect flow".

  Step 2: The victim informs the immediate upstream node where the suspect flow is coming from. This upstream node then processes suspect flow through a "virtual queue." Packets in this virtual queue are transmitted to the victim node with probability p1 and are otherwise held. This decreases the flow rate of suspect packets by a factor p1.

  Step 3: If the high flow rate is not due to an attack, then normal congestion control mechanisms will signal the packet sources to slow down and the buffer content at the "victim node" will begin to decrease. If this occurs and the content drops below some threshold T2, the system resets to a "normal" mode.

  Step 4: If there is a real DoS attack (i.e., the attacking nodes do not respond to congestion control messages), then the "virtual queue" will build up. When a threshold V1 is exceeded, this node informs the immediate upstream node where the suspect flow comes from and a procedure similar to that described above is initiated. Through this "pushback" mechanism, the node(s) where the attack originates is eventually identified and cut off.

  This scheme has the benefit of promptly preventing buffer overflows, thus protecting innocent flows from excessive packet losses. It also identifies the node responsible for the attack and can do so for multiple distributed attacks, one at a time. We have also investigated implementation implications of this approach and means of adjusting the critical control parameters mentioned above: T1 and T2 at the victim node, and (pi, Vi) for

all upstream nodes i = 1,2,… This can be accomplished using Perturbation Analysis (PA) and Stochastic Fluid Models (SFM) as described elsewhere in the report.

- **Stochastic Fluid Models (SFM) for fast decision making:** Stochastic Fluid (or Flow) Models (SFMs) provide an alternative framework to detailed packet-by-packet modeling techniques. In a SFM, we view the movement of packets as a "flow" but we also treat the corresponding flow rate as a random process. This approach provides a very promising modeling framework for complex networks that not only accelerates simulation by orders of magnitude, but it also facilitates the use of network management methods that can be implemented in a real time setting (Panayiotou, Cassandras, Sun, and Wardi, 2004; Yu and Cassandras, 2005).

  SFMs facilitate the use of Perturbation Analysis (PA) methods that were originally developed for detailed queueing network models. PA methods efficiently and non-intrusively extract sensitivity information from observed data in a network; this information can then be combined with standard stochastic gradient-based optimization schemes to continuously adjust network parameters so as to optimize (or at least constantly improve) specific quality of service metrics. In the case of the feedback-based defense mechanism against Distributed DoS attacks that we have developed (described elsewhere in this report), the use of SFMs and PA provide the means for fast and simple sensitivity estimation of performance with respect to various controllable parameters (Wu and Cassandras, 2005). In more general settings, we have demonstrated how PA sensitivity estimators can be derived and have established their unbiasedness properties in multiclass settings (Cassandras, Sun, Panayiotou, and Wardi, 2003; Sun, Cassandras, and Panayiotou, 2004a), in multi-node models (Sun, Cassandras, and Panayiotou, 2004b), and in networks with feedback control which was never possible in traditional queueing models (Yu and Cassandras, 2004; Yu and Cassandras, 2006).

- **Randomized policies as a defense mechanism to computer/network attacks:** We have shown that in some simple tractable cases randomizing network operating policies (e.g., for routing purposes) causes minimal performance degradation under normal conditions, while performing significantly better under attack. We have thus tackled the problem of determining optimal randomized routing policies for a class of wireless networks in order to provide protection against attacks that can compromise a node and then easily falsify cost information used by common routing protocols. For example, a "sink-hole attack" compromises a node and broadcasts a fake low cost to neighboring nodes, thus enticing all such nodes to route packets to it. The neighboring nodes in turn broadcast the low cost of the compromised node to their neighbors and the end effect is that this node acts as a sink hole for all packets while also draining the energy of the wireless nodes. In order to reduce the effect of such attacks, probabilistic routing is an attractive alternative, since this makes it difficult for attackers to identify an "ideal" node to take over. We have developed such a randomized routing policy for wireless sensor networks where the objective is to maximize the lifetime of the network. We have shown (Wu and Cassandras, 2005) that there exists an optimal policy consisting of fixed routing probabilities which may be obtained by solving a set of relatively simple nonlinear programming problems.

  Over the last year of the project, our work increasingly focused on the class of wireless sensor networks which have rapidly proliferated and whose importance to both the military and civilian domains is quite obvious. Our most recent work has focused on such networks with real-time constraints and we have been able to develop simple algorithms for operating such networks and guaranteeing that these real-time constraints are not violated (Miao and Cassandras, 2007; Mao, Cassandras, and Zhao, 2007).

- **Intrusion detection and defense in wired and mobile wireless settings:** Because human behavior shows much regularity, activities on computer networks also show much regularity. Learning these regularities and detecting deviations from these regularities can identify attacks and misuse. This is the goal of intrusion and misuse detection. Particular focus areas during this past reporting period have been on insider attack and Mobile Ad-Hoc Networks (MANET).

  Insider attack, where authorized users (employees), maliciously misuse a system to cause disruption or to disclose secret information or steal information assets presents a substantial threat to the military and companies such as banks. In (**Pepyne, Hu, and Gong, 2004**) we proposed a novel misuse detection scheme based on queueing theory and logistic regression to detect insider attack in a class of users such as bank tellers that we call "transaction-based" users. For this class of users, normal behaviors are well defined and quite specific, which allows for the creation of user profiles against which a users behavior can be compared and evaluated for anomalies with high reliability.

  The new "network centric" military is making increasing use of MANETs as is civilian emergency response. A major problem in MANETs is protecting the routing protocols — corrupt the routing protocols and there is no way for information to find its way from source to destination through the network. (**Huang and Lee, 2004**) develops a

new framework for detecting routing anomalies in MANETs. In our framework, we begin with the idea that any attack in MANETs can be expressed as some combination of basic anomalous events. Thus, we first define a taxonomy of anomalous basic events. We then model the normal behavior of routing protocol operations using an Extended Finite State Automata (EFSA) model. The statistical and temporal features on the states and transitions of the EFSA are constructed using a machine learning approach. The EFSA is then employed to detect anomalous basic events that directly violate the statistical and temporal specifications that the model defines.

- **Advanced Bayesian networks for distributed monitoring, vulnerability assessment, and dynamic defense:** It is becoming evident that very few of the more sophisticated attacks in information networks can be detected or effectively handled by individual network nodes acting alone. Rather network security is a collaborative effort, or as they say "it takes a village." To address this there is a critical need for distributed monitoring and detection methods.

  Using advanced concepts in Bayesian networks, we are developing a novel object-based probabilistic reasoning framework for propagating and fusing noisy belief alerts from multiple distributed security sensors in information networks. We have designed a three-layer network to integrate network-wide information and provide early detection of attacks. At the lowest level, information from multiple intrusion detection systems at a single node is integrated, to form a higher-level belief about the probability of an attack on the node. On the middle level, information from multiple nodes in a subnet is integrated, to detect coordinated attacks against a site. On the highest level, network-wide information is integrated to form beliefs about the network as a whole.

  In this framework each participating node maintains a belief (probability distribution) about the security state of the network. The entire network forms a very large-scale, highly distributed Bayesian network. In addition, because the state of the network changes dynamically, the Bayesian network must take into account dynamic information. To accomplish this, we have developed a new, distributed, form of dynamic Bayesian networks called *asynchronous dynamic Bayesian networks*. These are networks that are fully distributed and take into account the system dynamics. Each node updates its beliefs asynchronously. Beliefs are updated based on local information at the node, the previous state of the node and system dynamics. Beliefs are then propagated to the neighbors of the node, which take them into account in forming their own beliefs. At any point in time, the set of beliefs at all the nodes approximates the probability distribution over the current state of the network, given all the observations that have occurred so far.

  In previous work, we developed a static version of this framework that does not take into account system dynamics. Our work laid a solid foundation for distributed monitoring by demonstrating the belief propagation approach in an asynchronous, heterogeneous setting. Our results have shown that the method is robust to random node failures and is capable of tracking rapid changes in environmental conditions (**C. Crick and A. Pfeffer, 2003**). The next step in analyzing asynchronous dynamic Bayesian networks is to determine whether they enjoy the same good robustness and convergence properties.

- **A manuscript of a book on Ordinal Optimization** - result of a 14 year study of a new approach to optimization. See also previously submitted summary.

- **A probabilistic approach to solve early detection of distributed network attacks**. We have developed a new multi-tiered framework using Bayesian networks. The framework operates at three levels: the single-node level, the subnet level, and the network level. The single node level involves local monitoring such as intrusion detection. The result of the network at the single node is a local probability of intrusion. The subnet level combines evidences at the individual nodes, and is centralized. The network level is fully distributed and takes into account information from all the nodes and subnets.

  We have developed a new framework for distributed reasoning about beliefs, called Asynchronous Dynamic Bayesian Networks (ADBNs). In an ADBN, the joint probability distribution over the entire state of the network is decomposed locally in terms of individual probability distributions of nodes.

  Inference, which is fully distributed and asynchronous, is based on message passing. Each node sends messages to neighboring nodes summarizing its beliefs about the state of the network. Nodes integrate messages from neighbors to form new beliefs. The algorithm works using a continuous representation of time: no fixed time step needs to be used. We have found that ADBNs are much more accurate than corresponding synchronized algorithms, even though the synchronized algorithms have the advantage of utilizing a centralized clock.

(6) Listing of all publications and technical reports supported under this grant or contract. Provide the list with the following breakout, and in standard format showing authors, title, journal, issue, and date.

(a) Papers published in peer-reviewed journals

1. Cassandras, C.G., Sun, G., Panayiotou, C.G., and Wardi, Y., "Perturbation Analysis and Control of Two-Class Stochastic Fluid Models for Communication Networks", IEEE Trans. on Automatic Control, AC-48, 5, pp. 770-782, 2003.

2. Paschalidis, I.C., Y., Liu, Y., Cassandras, C.G., and Panayiotou, C.G., "Inventory Control for Supply Chains with Service Level Constraints: A Synergy between Large Deviations and Perturbation Analysis", Annals of Operations Research, 126, pp. 231-258, 2004.

3. Yu, H., and Cassandras, C.G., "Perturbation Analysis for Production Control and Optimization of Manufacturing Systems", Automatica, Vol. 40, pp. 945-956, 2004.

4. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis of Multiclass Stochastic Fluid Models", J. of Discrete Event Dynamic Systems, Vol. 14, 3, pp. 267-307, 2004.

5. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis and Optimization of Stochastic Flow Networks", IEEE Trans. on Automatic Control, AC-49, 12, pp. 2113-2128, 2004.

6. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Feedback-Controlled Stochastic Flow Systems", IEEE Trans. on Automatic Control, AC-49, 8, pp. 1317-1332, 2004.

7. Panayiotou, C.G., Cassandras, C.G., Sun, G., and Wardi, Y., "Control of Communication Networks Using Infinitesimal Perturbation Analysis of Stochastic Fluid Models", in Advances in Communication Control Networks, Lecture Notes in Control and Information Sciences, Vol. 308, pp. 1-26, (S. Tarbouriech, C.T. Abdallah, and J. Chiasson, Ed's), Springer-Verlag, 2004.

8. Yu, H., and Cassandras, C.G., "A New Paradigm for On-Line Management of Communication Networks with Multiplicative Feedback Control", in Performance Evaluation and Planning Methods for the Next Generation Internet, (A. Girard, B. Sanso, and F. Vazquez-Abad, Ed's), pp. 297-332, Springer-Verlag, 2005.

9. Miao, L., and Cassandras, C.G., "Optimality of Static Control Policies in Some Discrete Event Systems", IEEE Trans. on Automatic Control, AC-50, 9, pp. 1427- 1431, 2005.

10. Cassandras, C.G., and Li, W., "Sensor Networks and Cooperative Control", European Journal of Control, Vol. 11, 4-5, pp. 436-463, 2005.

11. Li, W., and Cassandras, C.G., "A Cooperative Receding Horizon Controller for Multi-Vehicle Uncertain Environments", IEEE Trans. on Automatic Control, AC-51, 2, pp. 242-257, 2006.

12. Li, W., and Cassandras, C.G., "Centralized and Distributed Cooperative Receding Horizon Control of Autonomous Vehicle Missions", J. of Mathematical and Computer Modeling, Vol. 43, 9-10, pp. 1208-1228, 2006.

13. Panayiotou, C.G., and Cassandras, C.G., "Infinitesimal Perturbation Analysis for Make-To-Stock Manufacturing Systems Based on Stochastic Fluid Models", J. of Discrete Event Dynamic Systems, pp. 109-142, 2006.

14. Yu, H., and Cassandras, C.G., "Perturbation Analysis and Feedback Control of Communication Networks Using Stochastic Hybrid Models", Nonlinear Analysis, Vol. 65, 6, pp. 1251-1280, 2006.

15. Miao, L., and Cassandras, C.G., "Receding Horizon Control for a Class of Discrete Event Systems with Real-Time Constraints", to appear in IEEE Trans. on Automatic Control, 2007.

16. Mao, J., Cassandras, C.G., and Zhao, Q., "Optimal Dynamic Voltage Scaling in Power-Limited Systems with Real-Time Constraints", to appear in IEEE Trans. on Mobile Computing, 2007.

17. Prahlad Fogla and Wenke Lee, “q-Gram Matching Using Tree Models”, IEEE Transactions on Knowledge and Data Engineering, Vol. 18, No. 4 (April 2006).

18. Guan, X.-H., C. Song, and Y.-C. Ho, “Constrained Ordinal Optimization – A Feasibility Based Approach,” submitted to the J. of Discrete Event Dynamic Systems, 2005.

19. Ho, Y.-C., ”On Centralized Optimal Control,” IEEE Trans. On Automatic Control, Vol. 50, No. 4, pp. 537-539, April 2005.

20. Ho, Y.-C., Q.-C. Zhao, and Q.-S. Jia, “Vector Ordinal Optimization,” JOTA, 2005.

21. Jia, Q.-S., Q.-C. Zhao, and Y.-C. Ho, “Selection Rules for Ordinal Optimization,” J. of Mathematical and Computer Modeling, 2005.

22. Song, C., X. Guan, Q.-C. Zhao, and Y.-C. Ho, “Machine Learning Approach for Determining Feasible Schedules of a Remanufacturing System,” in IEEE Trans. on Automation in Science and Engineering, 2005.

23. Gao, F. and Y.-C.Ho, “Random Approximated Greedy Search for Feature Selection,” Asian J. of Control, Vol.6, No. 3, September 2004.

24. Zou, C.C., W. Gong, D. Towsley, and L. Gao, “The Monitoring and Early Detection of Internet Worms," in IEEE/ACM Transactions on Networking.

25. Zou, C.C., D. Towsley, and W. Gong, “On the Performance of Internet Worm Scanning Strategies,” in Journal of Performance Evaluation.

26. Lin, S.-Y., C.-H. Lin, and Y.-C. Ho, “An Ordinal Optimization theory Based Algorithm for solving the Optimal Power Flow Problems with Discrete Control Variables,” IEEE Transactions on Power Systems, pp. 276-286, February 2004.

27. S.Y. Lin, C.H. Lin, and Y.C. Ho, “An Ordinal Optimization Theory Based Algorithm for solving the Optimal Power Flow Problems with Discrete Control Variables,” IEEE Transactions on Power Systems, pp. 276-286, February 2004.

28. Y. Liu and W. Gong, “On Fluid Queueing Systems with Strict Priority,” IEEE Transactions on Automatic Control, January 2004.

29. Y. Wu and W. Gong, “Error Analysis of Burst Level Modeling of Active-Idle Sources,” in ACM Transactions on Modeling and Simulation, 2004.

30. Yongguang Zhang, Wenke Lee, and Yi-an Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, in ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

31. Y. Ho, D. L. Pepyne, Q. Zhao, H. Liu, Q. Yu, and B. Dukes, “ProgramID,” IEEE Journal of Discrete Event Dynamic Systems, Volume 14, Issue 4, October 2004, 381 – 393.

(b) Papers published in non-peer-reviewed journals or in conference proceedings

1. Cassandras, C.G., "From Discrete Event to Hybrid Systems", Proc. of 2002 Intl. Workshop on Discrete Event Systems, pp. 3-8, October 2002.

2. Cassandras, C.G., "Stochastic Fluid Models for Communication Networks", Proc. of 17th Intl. Symposium on Computer and Information Sciences, pp. 8-11, October 2002.

3. Sun, G., Cassandras, C.G., and Panayiotou, C.G., "Perturbation Analysis of a Multiclass Stochastic Fluid Model with Finite Buffer Capacity", Proc. of 41st IEEE Conf. Decision and Control, pp. 2171-2176, Dec. 2002.

4. Cassandras, C.G., and Mookherjee, R., "Receding Horizon Control for a Class of Hybrid Systems with Event Uncertainties", Proc. of 2003 American Control Conf., pp. 5197-5202, June 2003.

5. Cassandras, C.G., and Mookherjee, R., "Properties of Receding Horizon Controllers for Some Hybrid Systems with Event Uncertainties", Proc. 2003 IFAC Conf. on Analysis and Design of Hybrid Systems, pp. 413-418, June 2003.

6. Cassandras, C.G., and Mookherjee, R., "Receding Horizon Optimal Control for Some Stochastic Hybrid Systems", Proc. of 42nd IEEE Conf. Decision and Control, pp. 2162-2167, Dec. 2003.

7. Sun, G., Cassandras, C.G., Wardi, Y., and Panayiotou, C.G., "Perturbation Analysis of Stochastic Flow Networks", Proc. of 42nd IEEE Conf. Decision and Control, pp. 4831-4836, Dec. 2003.

8. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Feedback-Controlled Stochastic Flow Systems", Proc. of 42nd IEEE Conf. Decision and Control, pp. 6277-6282, Dec. 2003.

9. Yu, H., and Cassandras, C.G., "Perturbation Analysis of Stochastic Fluid Models with Multiplicative Feedback", Proc. of 2004 American Control Conf., pp. 5734-5739, June 2004.

10. Panayiotou, C.G., and Cassandras, C.G., "Infinitesimal Perturbation Analysis for Make-To-Stock Manufacturing Systems Based on Stochastic Fluid Models", Proc. of 2004 Intl. Workshop on Discrete Event Systems, pp. 247-252, Sep. 2004.

11. Wu, X., and Cassandras, C.G., "A Feeback Control Defense Strategy for Denial-of-Service Attacks", Proc. of 43rd IEEE Conf. Decision and Control, pp. 105-110, Dec. 2004.

12. Li, W., and Cassandras, C.G., "Stability Properties of a Receding Horizon Contoller for Cooperating UAVs", Proc. of 43rd IEEE Conf. Decision and Control, pp. 2905-2910, Dec. 2004.

13. Mao, J., Zhao, Q., and Cassandras, C.G., "Optimal Dynamic Voltage Scaling in Power-Limited Systems with Real-Time Constraints", Proc. of 43rd IEEE Conf. Decision and Control, pp. 1472-1477, Dec. 2004.

14. Yu, H., and Cassandras, C.G., "Multiplicative Feedback Control in Communication Networks Using Stochastic Flow Models", Proc. of 43rd IEEE Conf. Decision and Control, pp. 557-562, Dec. 2004.

15. Li, W., and Cassandras, C.G., "A Minimum-Power Wireless Sensor Network Self-Deployment Scheme", in Proc. of IEEE Wireless Communications and Networking Conference, 2005.

16. Miao, L., and Cassandras, C.G., "Optimality of Static Control Policies in Some Discrete Event Systems", Proc. of 2005 American Control Conf., pp. 1186-1191, June 2005.

17. Cassandras, C.G., and Li, W., "Cooperative Control Problems in the Deployment of Sensor Networks", in Proc. of Workshop on Modeling and Control of Complex Systems, June 2005.

18. Yu, H., and Cassandras, C.G., "Perturbation Analysis and Feedback Control of Communication Networks Using Stochastic Hybrid Models", in Proc. of 16th IFAC World Congress, July 2005.

19. Miao, L., and Cassandras, C.G., "Receding Horizon Control for a Class of Discrete Event Systems with Real-Time Constraints", Proc. of 44th IEEE Conf. Decision and Control, pp. 7714-7719, Dec. 2005.

20. Li, W., and Cassandras, C.G., "Distributed Cooperative Coverage Control of

21. Sensor Networks", Proc. of 44th IEEE Conf. Decision and Control, pp. 2542-2547, Dec. 2005.

22. Wu, X, and Cassandras, C.G., "A Maximum Time Optimal Control Approach to

23. Routing in Sensor Networks", Proc. of 44th IEEE Conf. Decision and Control, pp. 1137-1142, Dec. 2005.

24. Miao, L.., and Cassandras, C.G., "Optimal Transmission Scheduling for Energy-Efficient Wireless Networks", Proc. of IEEE INFOCOM'06, April 2006.

25. Mao, J., and Cassandras, C.G., "Optimal Control of Two-Stage Discrete Event Systems with Real-Time Constraints", Proc. of 2006 Intl. Workshop on Discrete Event Systems, pp. 145-150, July 2006.

26. Mao, J., and Cassandras, C.G., "Optimal Control of Multi-Stage Discrete Event Systems with Real-Time Constraints", Proc. of 45th IEEE Conf. Decision and Control, pp. 1057-1062, Dec. 2006.

27. Ning, X., and Cassandras, C.G., "Dynamic Sleep Time Control in Event Driven Wireless Sensor Networks", to appear in Proc. of 45th IEEE Conf. Decision and Control, pp. 2722-2727, Dec. 2006.

28. Miao, L., and Cassandras, C.G., "Structural Properties of Optimal Uplink Transmission Scheduling in Energy-Efficient Wireless Networks with Real-Time Constraints", Proc. of 45th IEEE Conf. Decision and Control, pp. 2997-3002, Dec. 2006.

29. Y. Huang, W. Gong, D. Gupta, "MCMSDA: A Multi-Channel Multi-Sector Directional Antenna Wireless Lan", in proceeding of IEEE WOWMOM 2006, Buffalo, NY, June 26-29, 2006.

30. Monirul Sharif, George Riley, and Wenke Lee, “Comparative Study between Analytical Models and Packet-Level Worm Simulations”, in Proceedings of The 19th Workshop on Parallel and Distributed Simulation (PADS 2005), Monterey, CA, June 2005.

31. Y. Huang, W. Gong, D. Gupta, "Architecture and scheduling algorithm for a multi-channel wireless infrastructure network with diversity management layer", in proceeding of 44th IEEE Conference on Decision and Control, Dec, 2005.

32. Chen, X., H. Bai, L. Xia, and Y.C. Ho, “Target Detection in Randomly Distributed Sensor Networks,” in preparation.

33. Huang Y., and W. Lee, “Hotspot-Based Traceback for Mobile Ad Hoc Networks,” *Proc. of the 2005 ACM Workshop on Wireless Security* (WiSe 2005), Cologne, Germany, September 2005.

34. Pfeffer, A., and T. Tai, “Asynchronous Dynamic Bayesian Networks,” *Proc. of the 20st Conf. on Uncertainty in Artificial Intelligence*, 2005.

35. Zou, C.C., D. Towsley, W. Gong, and S. Cai, “Routing Worm: A Fast, Selective Attack Worm based on IP Address Information,” 19th *ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation* (PADS'05), June 2005.

36. Ho, Y.-C. and D.L. Pepyne, "A Conceptual Framework for Optimization and Distributed Intelligence," *Proc. of the 43rd IEEE Conf. on Decision and Control*, December 2004.

37. Zou, C.C., N. Duffield, D. Towsley, and W. Gong. "Adaptive Defence Against Various Network Attacks," *SRUTI: Steps to Reducing Unwanted Traffic on the Internet*, July 2005.

38. Zhang, Y., Y. Huang, and W. Lee, “An Extensible Environment for Evaluating Secure MANET,” *Proc. of the 1st IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, September 2005.

39. Zou, C.C., D. Towsley, and W. Gong, "Email Worm Modeling and Defense,”13th *International Conference on Computer Communications and Networks* (ICCCN'04), October 2004.

40. S. Cai, L. Gao, W. Gong, and W.-Q. Xu, "On Generating Internet Hierarchical Topology," in the *Proceedings of IEEE Conference on Decision and Control* (CDC) 2004.

41. S. Cai, Y. Liu and W. Gong, "Client-Controlled Slow TCP and Denial of Service,” in *Proceedings of IEEE Conference on Decision and Control* (CDC) 2004.

42. D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levin, and H. Owen, “HoneyStat: Local Worm Detection Using Honeypots,” in *Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection* (RAID 2004), French Riviera, France, September 2004.

43. H.H. Feng, J.T. Giffin, Y. Huang, S. Jha, W. Lee, and B.P. Miller, “Formalizing Sensitivity in Static Analysis for Intrusion Detection,” in *Proceedings of The 2004 IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.

44. G. Gu, D. Dagon, X. Qin, M.I. Sharif, W. Lee, and G.F. Riley, “Worm Detection, Early Warning, and Response Based on Local Victim Information”, *Proc. of the 20th Annual Computer Security Applications Conference* (ACSAC 2004), Tucson, Arizona, December 2004.

45. Ho, Y.-C. and D.L. Pepyne, "A Conceptual Framework for Optimization and Distributed Intelligence," *43rd IEEE Conference on Decision and Control*, 2004.

46. Y. Huang and W. Lee, “Attack Analysis and Detection for Ad Hoc Routing Protocols,” in *Proceedings of The 7th International Symposium on Recent Advances in Intrusion Detection* (RAID 2004), French Riviera, France, September 2004.

47. D. Pepyne, J. Hu, and W. Gong, "User Profiling for Computer Security," *Proc. of the American Control Conference*, Boston, MA, June 30-July 2, 2004.

48. G.F. Riley, M.I. Sharif, and W. Lee. “Simulating Internet Worms”, *Proc. of the 12th Annual Meeting of the IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS),* Volendam, The Netherlands, October 2004.

49. C.C. Zou, D. Towsley and W. Gong. "Email Worm Modeling and Defense,” in *13th International Conference on Computer Communications and Networks* (ICCCN'04), October 11-13, Chicago, 2004.

50. Zhou, T., Q. Yu, and H. Liu, “Comparison of Wireless Security Protocols,” *Proc. of the Int. Conf. on Computer, Communication and Control Technologies (CCCT’03)*, Orlando, FL, 2003.

51. C. Crick and A. Pfeffer, “Loopy Belief Propagation as a Basis for Communication in Sensor Networks,” *Conf. on Uncertainty in AI*, 2003.

52. A. Shrestha, L. Xing, and H. Liu, “Application Communication Reliability of Wireless Sensor Networks”, Proceedings of The 12th ISSAT International Conference on Reliability and Quality in Design, August 3-5, 2006, Chicago, Illinois.

53. Q. Yu and H. Liu, “Denial-of-Service Countermeasure with Immunization and Regulation,” IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005), Athens, Greece, 5-9 September 2005.

54. R. Suryanarayanan, L. Xing, and H. Liu, "Delay Reliability Analysis of a DiffServ Router," Proceedings of IASTED International Conference on Communications and Computer Networks, Cambridge, MA, 8-10 November 2004, pp. 362-367.

55. Q. Yu, S. Sharma, and H. Liu, "Handling Denial-of-Service Attacks with Quality-of-Service Framework," CNIS 2003: IASTED International Conference on Communication, Network, and Information Security, December 10 - December 12, 2003, New York, New York.

56. T. Zhou, Q. Yu, and H. Liu, "Comparison of Wireless Security Protocols," CCCT 2003: International Conference on Computer, Communication and Control Technologies, July 31 - August 2, 2003, Orlando, Florida.

(c) Papers presented at meetings, but not published in conference proceedings

1. Cassandras, C.G., “Vulnerability Assessment Tools for Complex Information Networks”, ARO Grantee Meeting, Cambridge, MA, May 2002.

2. Cassandras, C.G., “Hybrid Systems, Complexity, and Networking”, NSF-European Union Workshop on Advanced Hybrid Systems Theory for the Control of Networked Systems, Barcelona, Spain, July 2002.

3. Cassandras, C.G., “Joy and Perils of Automation”, NSF National Workshop for High School Teachers of Math and Science, Denver, CO, June 2003.

4. Cassandras, C.G., “Introduction to Hybrid Systems”, Intl. Summer School on Hybrid Systems, Veldhoven, The Netherlands, June 2003.

5. Cassandras, C.G., “Detecting and Reacting to DoS Attacks”, ARO Grantee Meeting, Cambridge, MA, July 2003.

6. Cassandras, C.G., “Cybersecurity”, Cyberposium 2004, Harvard Business School, Cambridge, MA, January 2004.

7. Cassandras, C.G., “Stochastic Fluid Models and Complexity Reduction”, Workshop on Recent Advances in Algebraic Systems and Control Theory, Atlanta, GA, January 2004.

8. Cassandras, C.G., “The Sensor Network Puzzle”, Emerging Technologies Workshop, Boston, MA, May 2004.

9. Cassandras, C.G., “Sensor Networks and Elevator Control for Optimizing Building Evacuation”, NIST Workshop on Building Security, Gaithersburg, MD, June 2004.

10. Cassandras, C.G., and Wu, X., “A Feedback Control Defense Strategy for DoS Computer Attacks”, ARO Grantee Meeting, Cambridge, MA, July 2004.

11. Cassandras, C.G., “A View of Cooperative Control for Autonomous Vehicles and Sensor Networks”, 2005 International Symposium on Intelligent Control, Limassol, Cyprus, June 2005.

12. Cassandras, C.G., “Discrete Event and Hybrid Systems”, IFAC Milestone Session, 16th IFAC World Congress, Prague, Czech Republic, July 2005.

13. Cassandras, C.G., and Wu, X., “Randomized Policies for Exploiting the Security-Performance Tradeoff in Wireless Networks”, ARO Grantee Meeting, Cambridge, MA, August 2005.

14. Cassandras, C.G., “Distributed Cooperative Coverage Control Using Sensor Networks”, Workshop on Distributed Sensor Networks, Los Alamos, NM, March 2006.

15. Cassandras, C.G., and Zhuang, S., "Dynamic Voltage Scaling for Power-Limited Systems with Hard and Soft Real-Time Tasks", 2006 INFORMS Annual Meeting, Pittsburgh, PA, November 2006.

(d) Manuscripts submitted, but not published

1. Zhuang, S., and Cassandras, C.G., "Optimal Control of Discrete Event Systems with Weakly Hard Real-Time Constraints", subm. to 2007 European Control Conf., 2006.

2. Mao, J., and Cassandras, C.G., "Optimal Control of Two-Stage Discrete Event Systems with Real-Time Constraints", subm. to J. of Discrete Event Dynamic Systems, 2006.

(e) Technical reports submitted to ARO

ALL OUR ANNUAL TECH. REPORTS TO DATE.

(7) List of all participating scientific personnel showing any advanced degrees earned by them while employed on the project

- David Pepyne (post doc)
- Jonathan Lee (ph.d),
- X.C. Lin (ph.d),
- Qing-Shan Jia (ph.d.)
- Changchun Zou (ph.d)
- Hanping Feng (ph.d)
- Songlin Cai (ph.d)
- Xiaoyi Wu (ph.d)
- Yi-an Huang (ph.d)
- Gang Sun (ph.d)
- Haining Yu (ph.d)
- Xiaoyi Wu (ph.d)
- Kirk Wesselowski (ph.d)
- Qin Yu (M.S.)
- Ying Liu (M.S.)

(8) Report of Inventions (by title only)

Virtually all of our work is presented at major conferences or published in major technical journals. In addition, our work has gained the attention of the news media, government leaders (in the Army, SPAWAR, DARPA, and NSF), Internet service providers, and network equipment manufacturers. In addition, several of our members work with industry (AT&T, MIT Lincoln Labs, Genuity, Tellabs), law enforcement (New England Electronic Crimes Taskforce), and other research organizations (Institute for Information Infrastructure Protection, I3P, Dartmouth College). In addition, this research program has served to directly support 1 undergraduate, 4 masters, and 7 Ph.D. students who have since gone on to faculty and research positions.

Our work on Internet worm detection and mitigation, wireless communications security, and intrusion detection algorithms has attracted significant attention from the news media, Army leaders, Internet service providers, and network equipment manufacturers. Our researchers have been interviewed for National Public Radio. Mr. J. Douglas Sizelove (DUSA-OR) has shown interest in our work on intrusion detection for insider attack. Dr. Phuong Nguyen of SPAWAR presented our work on worm detection and quarantine at DARPA. Several Internet service providers and equipment manufactures have shown interest in our feedback-based methods for traffic control.

We travel far and wide to disseminate our research results through numerous presentations given at international conferences, academic institutions, industry, government, law enforcement, and professional organizations.

Additionally, our members frequently consult with the IT offices at our various institutions, with industry (MIT Lincoln Labs, Genuity, Tellabs), law enforcement (New England Electronic Crimes Taskforce), and other research organizations (Institute for Information Infrastructure Protection, I3P, Dartmouth College).

N United States Patent Application: "Adaptive Defense Against Various Network Attacks", Inventors: Zou, Duffield, Towsley, and Gong, AT&T Docket Number 2004-0511

(9) Bibliography

This project supports 7 senior researchers at 5 universities.

Yu-Chi (Larry) Ho (lead PI), T. Jefferson Coolidge Research Professor of Applied Mathematics and Gordon McKay Research Professor of System Engineering, *Harvard University*, Cambridge, MA. Prof. Ho received the S.B. and S.M. degrees in Electrical Engineering from M.I.T. and Ph.D. in Applied Mathematics from Harvard University. He has published more than 140 articles and three books. He is active on the editorial boards and editorial advisory boards of several international journals and is the editor-in-chief of the International *Journal on Discrete Event Dynamic Systems* (JDEDS). He is the recipient of many fellowships and awards including the Guggenheim (1970), the IEEE Field Award for Control Engineering and Science (1989), the Chiang Technology Achievement Prize (1993), the Bellman Control Heritage Award of the American Automatic Control Council (1999), and the ASME Rufus Oldenburger Award (1999). He is a Life Fellow of the IEEE, an inaugural Fellow of INFORMS (2002), a member of the U.S. National Academy of Engineering (1987), and foreign member of the Chinese Academy of Sciences (2000) and Chinese Academy of Engineering (2000).

Avrom (Avi) Pfeffer, Assistant Professor of Computer Science, *Harvard University*, Cambridge, MA. Prof. Pfeffer received the BA from Berkeley (1995) and Ph.D. from Stanford University (2000), both in Computer Science. His doctoral research on probabilistic reasoning for complex systems developed powerful, scalable languages and algorithms for reasoning under uncertainty. He has also published articles on machine learning, computational game theory, and database systems. He is co-inventor of object-oriented Bayesian networks and of learning with probabilistic relational models. Honors and awards include the Berkeley Departmental Citation (1995), an NSF Graduate Research Fellowship (1996), the UAI Best Student Paper award (1997), and an NSF Career Award (2001).

Christos G. Cassandras, Professor of Manufacturing Engineering and Professor of Electrical and Computer Engineering, *Boston University*, Brookline, MA. Prof. Cassandras received degrees from Yale University (B.S.), Stanford University (M.S.E.E.), and Harvard University (S.M.; Ph.D.). From 1982-84 he was with ITP Boston, Inc. where he worked on the design of automated manufacturing systems. From 1984-1996 he was a faculty member in the Department of Electrical and Computer Engineering at the University of Massachusetts-Amherst. He specializes in the areas of discrete event systems, stochastic optimization, and computer simulation, with applications to computer networks, manufacturing systems, and transportation systems. He has published over 200 papers and two textbooks in these areas. He has guest-edited several technical journal issues and serves on several editorial boards. Dr. Cassandras is currently Editor-in-Chief of the *IEEE Transactions on Automatic Control* and has served as Editor for Technical Notes and Correspondence and as an Associate Editor. He is a member of the IEEE Control Systems Society (CSS) Board of Governors, General Chair for the 2004 IEEE Conf. on Decision and Control, past chair of the CSS Technical Committee on Control Theory, and has served as Program Chair for various conferences. Prof. Cassandras is the recipient of the 1999 Harold Chestnut Prize (IFAC Best Control Engineering Textbook) for “Discrete Event Systems: Modeling and Performance Analysis”; a 1991 Lilly Fellowship; a member of Phi Beta Kappa and Tau Beta Pi; and a Fellow of the IEEE.

Weibo Gong, Professor of Electrical and Computer Engineering and Computer Science, *University of Massachusetts*, Amherst, MA. Prof. Gong received the Ph.D. from Harvard University. His research interests include statistical modeling for computer security, large data set analysis, network modeling and congestion control analysis. Prof. Gong is the founding Director of the Complex Systems Modeling and Control Laboratory at UMass. This lab researches information system security with support from government and industry. His research group has published more than 100 papers in journals and refereed conference proceedings. Dr. Gong has been on the editorial boards for several IEEE Transactions and is an Associate Editor for the *Journal of Optimization Theory and Applications*. He co-edited the book *Modeling, Control, and Optimization of Complex Systems* (Kluwer, 2002), and the *IEEE Trans. on Automatic Control* special issue on Systems and Control Methods in Communication Networks (June 2002). Dr. Gong is current Chair of the IEEE Control Systems Society (CSS) Network and Communication Technical Committee, and publications chair for the 2004 IEEE Conf. on Decision and Control. Prizes and awards

include the IEEE Transactions on Automatic Control, George Axelby Outstanding Paper Award (1997), University of Massachusetts-Amherst, College of Engineering Senior Faculty Award (2002). Dr. Gong is a Fellow of the IEEE.

David L. Pepyne, Senior Research Scientist, Consortium for Distributed Decision Making, *University of Massachusetts*, Amherst, MA; Consultant, Division of Engineering and Applied Science, *Harvard University*, Cambridge, MA. Dr. Pepyne has worked in law enforcement, as an officer in the U.S. Air Force, and as a project engineer in industry. He received the Ph.D. from the Dept. of Electrical and Computer Engineering, University of Massachusetts, Amherst (1999). He has published papers on learning, optimization, discrete event and hybrid systems, control design, electric power system protection and markets, and network security. He is an active member of the IEEE Control Systems Society (CSS), having served on the CSS Conf. Editorial Board (1999-2000) and Conf. on Decision and Control Organizing Committee (Publicity Chair, 2004). Awards include a DoD CIP/IA Fellowship (2001).

Wenke Lee, Assistant Professor, College of Computing, *Georgia Institute of Technology*, Atlanta, GA. Prof. Lee received the Ph.D. from Columbia University (1999). He is the inventor of MADAM ID (Mining Audit Data for Automated Models for Intrusion Detection), a component of JAM (Java Agents for Meta-Learning). The performance of the models produced by MADAM ID rated among the best in the 1998 DARPA Intrusion Detection Evaluation. Dr. Lee has published widely in leading security and data mining conferences. Honors and awards include an NSF Career Award (2002), best paper award (Applied Research category, 1999 ACM SIGKDD), and two runner up best paper awards (Applied Research Category, 1997 and 1998 ACM SIGKDD).

Hong Liu, Professor, Dept. of Electrical and Computer Engineering, University of Massachusetts at Dartmouth, MA. Prof. Liu received the B.S. (with Honors) in Computer Science and Mathematics and the M.S. in Computer Science, both from Hefei Polytechnic University, China. She won State Third Award for her master thesis and graphics research. Prof. Liu received her Ph.D. in Computer Science from the Polytechnic University of New York (formerly known as Brooklyn Polytechnic). From 1987-1990, Dr. Liu was a faculty member at Brooklyn Polytechnic. She joined the faculty at UMass Dartmouth in 1990, where she is now a Professor. Her research interests are computer networks, compilers, and programming languages. Honors and awards include a Brownstein Doctoral Research Award, a Westinghouse Research Grant for Women in EE/CS, and an NSF/GOALI Award. Dr. Liu is an active liaison to the computer networking industry, she is a member of the IEEE, IEEE Communications Society, ACM, ACM SIGCOMM, and Upsilon Pi Epsilon.

(10) Appendixes

None.